X9007 – ACCESS CONTROL SYSTEM

DESCRIPTION

PART 1 - GENERAL

1.1 SCOPE OF WORK

The following scope of work shall be included in this contract and does not necessarily include every item of work. The Contractor shall supply and install items that meet the specified requirements of the final order. The Security Management System (SMS) Workstations shall be furnished complete, installed, tested, and operational. The SMS is designed to secure the designated facilities. The work to be provided, in addition to designing, furnishing, and installing the SMS, shall include the following:

Provide Software that meets specified contract requirements. Verification that proposed equipment and devices furnished are adequate for the intended purpose.

Perform a layout check to ensure that adequate access is available for construction, installation, and maintenance of equipment and devices furnished; however, the Contractor is not responsible for furniture. The Contractor shall consult the owner/engineer in the design of the workplace.

Perform acceptance tests to show system is properly installed and that it meets the specifications and applicable codes.

The Airports System Administrator shall be responsible to configure and maintain the system. System utilities shall be provided for the System Administrator to use. Software for backups and log file maintenance shall also be provided.

The Contractor shall provide specific training manuals for system administrators, managers and guards.

1.2 SCOPE OF SYSTEM

1.2.1 Basic System Characteristics

1.2.2 Specific Manufacturer

1.2.2.1 This specification is based on the capabilities of Andover Controls' XPress Integrated Security Management System. Any alternate system shall comply with all of the capabilities of the specified system and be pre-approved by the specifying engineer.

1) The SMS shall provide an integrated solution through the use of control hardware and PC workstation-based software for Access Control, Security/Intrusion Detection, and Photo Imaging.
2) This SMS shall provide a true multi-tasking PC-based platform running Microsoft's Windows 2000 Workstation.
3) The SMS shall communicate with native TCP/IP Primary Network Controllers over an existing CUSTOMER-owned Ethernet TCP/IP enterprise network.

4) The SMS shall be capable of controlling a maximum of 28 doors, 5,000 cardholders (expandable to 78,000), and monitoring up to 250 supervised input points or outputs.

1.2.3 Base Bid

Contractor shall provide the SMS as shown on the drawings and specified herein including but not limited to the following:
Integrated Workstation
Workstation Peripherals
Primary Network Controller
LON I/O Modules
Field Hardware Devices
Software Required for Specification Operation

1.3 REFERENCED AND SYSTEM CERTIFICATIONS

Design and operation of the SMS shall conform to the following referenced codes, regulations, and standards as applicable:
National Electrical Code (NEC)
UL 294 Access Control Systems
Designed ion accordance with UL 1076 requirements
FCC Rules and Regulations
Part 15, Radio Frequency Devices
National Electrical Manufacturers Association (NEMA)
Applicable Federal, State and Local laws, regulations, codes
Americans with Disabilities Act (ADA)

1.4 QUALITY ASSURANCE

1.4.1 Manufacturer

1.4.1.1 Company specializing in Security/Access Control and CCTV Systems with a minimum of two years experience.

1.4.2 Installer

1.4.2.1 Company specializing in Security/Access Control and CCTV Systems with a minimum of five years experience.

1.5 SUBMITTALS

Contractor shall submit all items in accordance with the requirements of Section 1, Submittals, and shall include, but not be limited to the following:

Model numbers of all components furnished on the job
Manufacturer’s installation instructions
Input power requirements for all components
Complete engineered drawings indicating:
Layout, wiring diagrams, and dimensions
Point-to-point wiring diagrams for all devices

Termination details for all devices
Single-line system architecture drawings representing the entire system
Operation Data: Include operating instructions in the form of at least three training manuals – one for system administrators, one for managers, and one for guards.
Maintenance Data: Include maintenance and repair procedures
Training Syllabus: Include course outlines for each of the end user training programs. The course outlines shall include the course duration, location, prerequisites, and a brief description of the subject matter.

1.6 GUARANTEE

1.6.1 Period

The Contractor shall guarantee all labor, workmanship and materials for a period of 1 year from the date of final acceptance as evidenced by receipt of a signed acceptance certificate from Waukesha County. Should a failure occur within the first year to the system, the Contractor shall provide all labor and materials necessary to restore the system to a complete operating condition, at no cost to the Owner. The Contractor shall provide a lifetime guarantee on proximity cards. All cards that crack or de-laminate during normal service shall be replaced at no cost to the owner.

1.7 SYSTEM DESCRIPTION & CAPABILITIES

1.7.1 Primary Function

The SMS's primary function shall be to regulate access through specific doors and gates to secured areas within the airports facility. The system shall offer photo imaging as an option. The SMS shall utilize a single database for its access control, and photo imaging functionality. This integration shall be provided under one operating environment. The SMS's workstation environment shall be Microsoft Windows 2000 Workstation operating system. No alternates will be accepted.

1.7.1.1 The software architecture shall be object-oriented in design, a true 32-bit application suite utilizing Microsoft's Active X technology.

1.7.1.2 The SMS shall allow the configuration of an integrated workstation that provides both alarm display and monitoring, as well as capture, playback, and storage of video. This workstation and Primary Network Controller shall be connected via the airports 10 Mbps Ethernet backbone using the TCP/IP protocol.

1.7.1.3 The Primary Network Controllers shall support multiple communication ports including a LON communications network from which up to 32 I/O modules shall connect.

1.7.1.4 The Integrated Workstation shall be able to monitor field hardware devices such as card readers and I/O modules, display alarm and event activity, and provide both pre- and post-event video. Administrative tasks such as assigning areas, schedules, report generation, displaying color graphic maps, etc., shall also be available.

1.7.1.5 The Integrated Workstation with the Photo Imaging option shall serve as both the credential creation and data input Workstation for the cardholder management of the system. The integrated workstation shall allow all the functions of a photo imaging, and an alarm and display monitoring Workstation.

1.7.1.6 The SMS shall utilize a commercially available Open Database Connectivity (ODBC)-compliant open architecture relational database with flexible design allowing the integration into other data structures. This database shall handle the storage and retrieval of all cardholder record information, images, system maps, reports, screen designs, and video. The database shall operate in a truly multi-tasking environment without degradation of system operation and be of a design that will handle the transaction loading placed on the system. The relational database shall support on-line backup, and stored procedures with control logic. The system database shall contain all point configurations and programs in each of the controllers that have been assigned to the network. Systems based on MS Access or a proprietary database management system are not acceptable.

1.7.2 System Design

The SMS shall be designed to perform a wide variety of features and functions. These system functions shall be categorized into five (5) primary "system departments" which shall include:

1.7.2.1 Access Control

The system shall be able to make access granted or denied decisions, define access privileges, and to set schedules and holiday groups. The system shall support features such as area control, anti-pass back, and extended shunt time in-line with ADA requirements.

1.7.2.2 Alarm Management

A color graphic application shall allow a user to create or import customized color graphic maps of their facility and to attach alarm icons to those maps. Alarms shall be prioritized. A status window shall provide information about the specific alarm including date and time and location of the alarm. The SMS shall allow unique emergency instructions to be specified for each type of alarm. It shall be possible to e-mail each alarm to any recipient listed in the workstation's e-mail address book. An alarm journal shall be available to log important daily events.

1.7.2.3 Cardholder Management and Enrollment

This employee management functionality shall allow the enrollment of cardholders into the database and capturing of images with the photo imaging option. This functionality shall also allow the user to assign or modify access privileges of a cardholder.

The SMS shall optionally include a credential creation and production system integrated with the cardholder management system. This shall allow the creation of different badge types based on database fields and the use of security colors to allow security staff to quickly identify personnel access authority by the badge design.

1.7.2.4 System Administration

System Administration tasks such as defining workstation and user permissions, area access, schedules, generation of reports, displaying maps, etc. shall be available. System tape back-up and remote diagnostics shall be included.

PART 2 – OPERATIONAL REQUIREMENTS

2.1 GENERAL

The design of the SMS shall include devices and equipment used to monitor and control access to restricted areas, detect and deny unauthorized entries within specific buildings or areas, annunciate alarms, and generate reports. The SMS is to be designed and configured to provide operational flexibility and reliable performance.

2.1.1 Functional Responsibilities

Airport shall have the responsibility for managing and operating the system, as well as maintaining the graphical representations of the designated facility input into the system's color graphics application. It shall be the responsibility of the airport to enroll all personnel and capture the associated images, if applicable.

2.1.2 Operational Concept

The SMS shall consist of equipment and devices placed at predetermined locations to ensure that only cardholders who are authorized to enter secured areas through certain doors or gates can do so and that certain defined events can be viewed and captured digitally for review. This shall be accomplished by means of a computer and electronic devices used in conjunction with door locks, gate systems, card readers, and closed circuit television cameras.

2.1.2.1 When an employee is newly hired or is changing job responsibilities, a personnel form shall be available within the SMS application. This employee data screen shall contain 20 data entry fields of information. These fields shall vary in character length as dictated by the system.

2.1.2.2 The SMS shall provide a fully integrated link between the Access Control, Alarm Monitoring, and Photo Imaging. This shall allow specific information concerning personnel data to be automatically shared by utilizing a single database. Personnel data and images shall be enrolled and captured via the photo imaging application and access privileges shall be assigned via the access control application.

2.1.2.3 After the applicant's picture is captured by the system, if applicable, the photo image is to be printed on the badge and appear in a pre-defined format specified prior to the system installation.

2.2 SMS FEATURES

All SMS applications shall be easy, quick, and efficient to use. The system shall combine keyboard and mouse operations with graphical presentations of screen information. All routine information displayed and requiring input shall be in English language prose. No operation shall require the interpretation of machine code or the use of mnemonics.

2.2.1 Access Control

2.2.1.1 Access Privileges – All cardholders shall have facility access based on privileges assigned by controlled area, time, and date. The time zones for each day shall be pre-defined by airport and shall be able to be modified quickly by authorized employees without vendor intervention.

2.2.1.2 Holidays - The Holidays application shall allow the System Administrator to create holiday schedules that designate individual days as holidays, or special days to cover vacations, maintenance shutdowns, or other events, indefinitely into the future. Holidays or special days shall signal that the system operate on a schedule different from the normal schedule. The system shall not limit the number of holiday or special schedules that can be created.

2.2.1.3 Time/Date – The time and date of the system shall be set y the operating system of the client workstation. Dates for Daylight Savings Time shall automatically take effect. Holiday schedules shall be capable of overriding normal schedules in effect.

2.2.1.4 Shunt Time – A Shunt Time feature shall be provided to allow users to program, at the door level, a length of time to hold a door open without creating an alarm condition at the monitoring workstation. An active input control window shall be available to easily permit manual override of assigned inputs.

2.2.1.5 Manual Control – A user shall have the ability to easily dictate manual control of all doors connected to the system via an active door control window.

2.2.2 Alarm Management

2.2.2.1 General

The software shall be capable of accepting alarms directly from controllers, or generating alarms based on polling of data in controllers and comparing to limits or conditional relationships configured through the software. The system shall offer the following:

1) A minimum of 255 alarm notification levels.
2) Automatic logging in the database of the alarm message.
3) Automatic printing of the alarm information or alarm report to an alarm printer or report printer.
4) Sounding of an audible beep or playing an audio (.wav) or displaying a video (.avi) file on alarm initiation or return to normal.
5) An active alarm viewer which can be customized for each user or user type to hide or display any alarm attributes.

6) An active alarm viewer that can be configured for critical alarms such that a user can type in text in an alarm entry field and/or pick from the user action drop-down list.
7) The ability to Soft-acknowledge (Silence) or Acknowledge the alarm.
8) The ability to highlight a specific alarm and select a button to display an associated graphic map, or select button to display an associated report.
9) The ability to display all other alarms while any one alarm is being addressed.
10) Alarms shall be able to be e-mailed to designated recipients listed in the workstation's e-mail address book.

2.2.2.2 Current Status Indication

The active alarm view shall provide a status indicator that displays the current status of alarms and field controllers.

2.2.2.3 Cardholder Recorder Call-up

The user shall be able to initiate the call-up of a cardholder record.

2.2.2.4 Scheduling

Time of day schedules shall be in a calendar style and shall be programmable up to year 2106.

2.2.3 Cardholder Management and Enrollment

The SMS shall generate and store up to 5,000 personnel records (expandable), and monitor badge/credential use. An optional SMS photo imaging application may produce credentials based on data and images that are input and captured at the time of enrollment. Credential images are to be digitized using industry standard JPEG image compression, and printed using a dye-sublimation/resin thermal transfer printing process that is of high quality and environmentally safe.

2.2.3.1 Create and Maintain Personnel Database

The user shall be able to create personnel records through direct input into the personnel record.

2.2.3.2 Assigning Access Privileges

After a badge is created, it shall be possible to assign access privileges to the personnel record using check boxes. When an individual's access privileges are modified, that change shall be propagated to the controller immediately upon completion of the change. Changes of access privileges shall affect only the modified record, and shall not record a download of the entire cardholder database.

2.2.3.3 Badge Creation

A. Image Capture

The SMS shall include all equipment required to capture a high quality portrait image, with flash lighting and a high quality RGB digital video camera. The SMS shall include the ability, upon command, to preview on-line and in full color, the badge as it will appear when printed. SMS image capture, storage, and hardware compression techniques shall be in compliance with JPEG standard.

B. Pre-defined Badge Formats

The badge format, including background color, layout, location of photo image, applicable graphics or company logos, text, etc., shall be completely automatically determined by the system based on employee record information.

C. Color Credential/Badge Printing

Credential printers shall be high-density dye-sublimation type printers offering 300 dots per inch resolution with a clear overlay option for high durability.

D. Batch Printing

The Airports Photo Imaging user shall be able to print a credential immediately or send it to a print queue. The SMS Photo Imaging Workstation shall have the ability to print a large volume of badges with a single command using a print queue screen. At the print queue, the user shall have the option of printing all badges, printing selected badges, deleting a badge, or previewing badges without printing.

2.2.3.4 Search Records

The SMS shall allow the user to search for records and images using search criteria on any field(s) in the database.

2.2.4 System Administration

2.2.4.1 General

The workstation software shall use a familiar Windows Explorer-style interface for a user to view and/or edit any object (controller, point, alarm, report, schedule, etc.) in the entire system.

2.2.4.2 Workstation and Password Privileges

The software shall be designed so that each user of the software can have a unique username and password. The SMS shall support individual password restrictions for each user.

2.2.4.3 Create and Maintain Door Objects

Door objects shall be easily enabled. The door object editor shall be tabular in design for easy navigation through the attribute fields.

2.2.4.4 User Administration and Roles

Any system user with user administration roles can create users and assign permissions to them.

2.2.4.5 Alarm Zone Configuration

The SMS shall allow control of which cameras shall be recorded during an alarm event and defines the type of event that triggers recording. Each alarm zone shall be able to be configured individually.

2.2.4.6 Reports

The SMS shall have an integrated report writer pre-configured with all common access control reporting requirements. At a minimum the system must provide the reporting capability to view access event, alarm, area/cardholder data and door and user-activity.

2.2.4.7 Custom Report Generation

The software shall contain a built-in custom report generator, featuring word processing tools for the creation of custom reports. These custom reports shall be able to be set up to automatically run or be generated on demand.

2.2.4.8 System Tape Backup

The SMS shall provide tape backup and restore programs utilizing the multi-tasking capabilities of the SMS system which run concurrent with all other application of the system and in no way shall inhibit other use of the terminal. Database backup shall occur dynamically while other alarm monitoring, Photo Imaging, access control and DVR applications remain active.

2.2.4.9 Color Graphic Map Configuation

The system shall have the ability to draw, edit, and copy site color graphic maps without using any third-party system software. The map configuration software shall import map drawings from the following formats at a minimum:

PEG (.JPG), Windows Bitmap (.BMP)

2.3 SMS DATA EXCHANGE

2.3.1 Data Import/Export

The SMS shall allow the end user, and/or Contractor, to create import and/or export scripts to/from the SMS.

2.4 SMS REDUNDANCY

2.4.1 Fault Tolerance

The system shall be fault tolerant in the event of the loss of the CPU, disk drives, or other hardware required to maintain the operational integrity of the system.

A single component failure in the system shall not cause the entire system to fail. System users shall be informed of any detectable component failure via an alarm event.

2.4.2 Distributed Intelligence

In the event system communications are lost or the Workstation fails, the Primary Network Controller (PNC) shall provide complete control, operation, and supervision of all monitoring and control points. The PNC shall be configured with a UPS battery that shall support the field controller for a minimum of 1 hour. The PNC shall be installed with enough memory to support 5,000 cardholders (upgradeable to 78,000). The SMS shall incorporate performance tests and precautions so as to avoid system failure. In the event of a failure, transactions are to be stored in a PNC FIFO buffer until the field controller comes back on-line, at which time the data is uploaded to a Workstation for reporting and storage. The PNC shall register as on-line with the Workstation when communications are re-established. A complete download of database and access information shall not be required because of off-line operation.

EQUIPMENT AND MATERIALS

PART 3 - PRODUCTS

3.1 SMS WORKSTATION REQUIREMENTS

The SMS shall wholly integrate all access control and Digital Video Recording functionality into a single workstation and database using a networked environment. The integrated workstation software shall be a single workstation system with built-in database. The Workstation shall be capable of residing directly on the CUSTOMER's Ethernet TCP/IP LAN/WAN with no required gateways. The Workstation shall be capable of using standard, commercially available off-the-shelf Ethernet infrastructure components such as routers and hubs. With this design the CUSTOMER may utilize the investment of an existing or new enterprise network or structured cabling system.

3.1.1 Computer Hardware

Unless otherwise stated, computer equipment needed for the workstation consists of the following minimum requirement:
900 MHz CPU with 512MB of RAM
Windows 2000 Workstation
250W Power Supply
Optional Redundant Power Supply
2-Port IDE RAID Controller
Two 40GB drives configured in RAID 1 (mirrored), with operating system drives on logical device "C:"

4U rack-mount chassis
10/100 CAT 5 Network Interface Card (NIC)
Optional 8U chassis with 6 additional drives can be supplied if additional local storage is required (2-port IDE replaced by 8-port card).

3.1.2 Integrated Workstation

The Integrated Workstation shall be provided with full Alarm Monitoring, and Photo Imaging functionality on a single workstation. The Integrated Workstation shall be the main alarm monitoring workstation, and used for configuring the access control features described in this specification. This workstation can be used for image capture, badge production, and employee enrollment with the Photo Imaging option.

3.1.2.1 Dot Matrix Printer

The event/report printer shall be a compact serial 9-pin dot matrix printer that will print text data in draft and NLQ modes.

3.1.2.2 Laser Printer

The laser printer shall be a parallel interface dry-type laser electro photographic process printer.

3.1.2.3 Digital ID Printer

The SMS shall provide a high density dye-sublimation/resign thermal transfer type image printing systems which prints two sides, edge to edge, directly onto a white-unfinished 0.030 PVC, PVH or PVCH card. The SMS shall download the badge layout directly to the printer and using a dye diffusion thermal transfer process print it directly onto the card.

3.2 SMS FIELD HARDWARE DEVICES

3.2.1 Overview

The SMS shall be equipped with the field hardware required to receive alarms, administer all access granted/denied decisions. The SMS field hardware shall be able to include any or all of the following features:

3.2.1.1 Real Time Clock (RTC)

A battery backed RTC shall provide the following information: time-of-day, day, month year, and day-of-week. The system shall automatically correct for daylight savings time and leap years.

3.2.1.2 Automatic Restart After Power Failure

Upon restoration of power, the controller shall automatically and without human intervention: update all monitored functions; resume operation based on current, synchronized time and status, and implement special start-up strategies as required.

3.2.1.3 Approval Listings

As a minimum, all controllers shall be listed to comply with UL Standard 294 and in-line with 1076 requirements, FCC, and CE.

3.2.2 Primary Network Controller

Primary Network Controller (PNC) shall provide overall system coordination, accept control programs, perform automated control functions and security management, and perform all necessary mathematical functions.

The PNC communication shall use the CUSTOMER's existing Ethernet network running at 10 MBPS. The PNC shall be a native TCP/IP device and shall not require use of terminal servers or other devices to allow direct Ethernet connectivity.

3.2.2.1 PNC shall be microprocessor-based and use real-time digital control processors. The control panel shall consist of modular hardware including power supply, CPU board, and input/output modules.

3.2.2.2 Memory

A minimum of 4MB of RAM with math coprocessor shall be provided for the Ethernet-based PNC. In addition, the controller shall contain a minimum of 4MV of 'Flash EEPROM' memory for the system firmware. Firmware shall be updated on-line. Use of EEPROM-based firmware requiring Waukesha County change-outs to perform upgrades is not acceptable.

3.2.2.3 Communication Ports

The Ethernet-based PNC shall utilize network communications and information management across a high speed Ethernet based network at 10 MBPS. The PNC shall be supplied to operate on Ethernet using the TCP/IP protocol. At a minimum, the PNC shall have built-in network communication error checking to the International Standard CRC16. Typical communication media shall be 10BaseT.

3.2.2.4 Networking

The network structure shall be transparent such that the controller may store and reference all global variables available in the network for use in the PNCs calculations or programs. The PNC shall also have access to any of the readers, card records, inputs, and outputs that are connected to it.

3.2.2.5 Power Supply

PNC shall operate from 100 to 240 VAC 50/60 Hz power. Line voltage below the operating range of the system shall be considered outages. The controller shall contain over voltage surge protection, and require no additional AC power signal conditioning.

3.2.2.6 Battery Back-Up

The PNC battery backup UPS circuit with built-in battery charger shall provide automatic battery backup UPS power in event of AC line failure. The PNC shall have a programmable battery backup providing choice of shutdown options including at least 72 hours of battery backup to maintain all volatile memory and real-time clock; or, this battery shall provide for full UPS operation for a minimum of 60 minutes.

3.2.3 Local I/O Modules

Local I/O modules shall be provided in a distributed or centrally located fashion. The I/O modules shall contain their own internal ROM, EEPROM, and SRAM. The I/O Modules shall maintain data integrity during a power failure through UPS or battery backed RAM.
Local I/O modules shall have the following:
Integrated testing and diagnostics for self-testing
Suitable interfaces and appropriate universal inputs and outputs for the connection of mechanical or electrical devices
Manual override facilities on all universal outputs for testing and commissioning purposes
Unique software address point on the network that does not require the manual setting of DIP or DIL switches
The I/O Modules shall cover the following range of types:
Access Control
Intrusion Detection and Digital Control

3.2.3.1 Networking

All modules shall be able to exchange information between other I/O
Modules and the Primary Network Controller during each field bus scan

3.2.3.2 Power Supply

The access control module shall be fed from a low voltage, 24 VDC power supply with battery backup, or from the power supply of the Primary Network Controller given adequate capacity.

3.2.4 Access Control Module

3.2.4.1 Description

Access Control I/O modules shall provide the interface for one card reader/keypad controlled door, to the Primary Network Controller. Each access controller shall include a Wiegand or ABA style card reader input, at least three supervised inputs for door status, exit request, and other inputs, and at least two relay outputs for the door lock and an optional auxiliary controlled point.

Each I/O module shall have the intelligence to perform all degrade-mode access control strategies stored in the I/O modules non-volatile EEPROM, without communication to other modules, in the event of a communications loss to the Primary Network Controller.

3.2.4.2 Input/Output

Inputs

The input section of the access I/O modules shall provide a minimum of 1 card reader channel and 1 keypad channel. It shall be possible to expand the number of card readers by simply adding I/O modules to the communications network. In addition, there shall be 3 supervised inputs on the base controller for request-to-exit devices, door status devices, and general supervised input monitoring.

The card reader inputs shall accept Proximity style readers. Each supervised input shall be able to distinguish among normal operation, a short, open circuit, or a fault. Inputs shall be able to use double resistor-based supervised circuits. The access control module shall support Wiegand output keypads.

Outputs

Output types shall be digital for control of doors. In addition to the door output, the control module shall contain one auxiliary output for ON/OFF control of annunciators, lights, etc. Outputs shall be available with built-in override switches.

The digital outputs shall be rated for 24 VAC/DC operation at 5 amps minimum. Each output shall have a corresponding LED for visual indication of its state.

A board-mounted 3-position switch shall be provided for each output allowing local overrides. The position of the switch shall be detectable in software and available for alarm annunciation. If override switches are not provided on board, external switches shall be provided and wired to include feedback and alarming of the switch position, and shall be mounted in a locked enclosure.

3.2.5 Intrusion Detection and Digital Control Module

3.2.5.1 Description

Intrusion Detection and Digital Control modules shall provide inputs and outputs to monitor and control non-reader-based system points, such as door contacts, motion sensors, gate actuators, etc.

3.2.5.2 Input/Output

Inputs

The Intrusion Detection Module shall provide 8 universal input points, using two-piece, removable screw terminal connectors.

Each supervised input circuit shall be able to distinguish among normal operation, a short, open circuit, or a fault. In addition, these same inputs can be configured for analog operation to monitor temperatures, humidity, or other parameters from transducers outputting industry standard signals of 0 – 5 VDC and 4 – 20 mA.

Outputs

The Digital Control Module shall provide 4 relay outputs, using two-piece, removable screw terminal connectors. The output type shall be digital using Form-C relays capable of switching 24 VAC/DC at 5 amps. Each output shall have a corresponding LED for visual indication of its state.

Outputs shall be available with built-in override switches. A board-mounted switch shall be provided for each output allowing local overrides. The position of the switch shall be detectable in software and available for alarm annunciation. If override switches are not provided on board, external switches shall be provided and wired to include feedback and alarming of the switch position, and shall be mounted in a locked enclosure.

3.2.6 Proximity Card Readers

Airport requires the SMS to provide HID, Motorola Indala, or Keri Proximity Card Readers or an approved equal. The product line shall offer a variety of readers to match airports needs. Each reader shall offer a low profile, rugged, weatherized polycarbonate sealed enclosure with multi-color LED's and a sounder for access granted and denied indications. Each shall be mountable indoor or outdoor.

3.2.7 Keypads

Keypads approved for the SMS shall be the Essex Electronics 12 Pad or approved equal. Keypads shall contain 3 columns by 4 rows containing the characters 0 through 9, the pound (#) and the star (*) sign. The keypads shall be suitable for either outdoor or indoor use.

3.2.8 Field Hardware Power Supplies

Power supplies for field hardware shall be compatible with the SMS equipment installed. Power supplies shall be regulated, linear and isolated versions for the field panels and other equipment. Each version shall be available in UPS with battery back-up and non-UPS models. All power supplies shall be housed in tampered, locked enclosures.

3.3 CREDENTIALS

3.3.1 General

The SMS System shall utilize card products designed specifically for security applications.

3.3.2 SMS Proximity Cards

Proximity shall be an access control/identification technology that utilizes radio frequency (RF) circuits in microchip form. The microchips are encoded and transmit the encoded information when activated.

3.3.3 SMS PVC Card

The SMS Contractor shall provide a credit card size (3.370" x 2.125" OD), or approved equal PVC (PVH or PVCH) card. Traditional paper media inserts shall not be acceptable.

CONSTRUCTION METHODS

4.1 INSTALLATION

Installation of the SMS shall include the appropriate equipment and shall be performed by a factory-trained Contractor Installer.

4.2 IMPLEMENTATION

Required planning and coordination of numerous elements and deliverables during the installation and commissioning phases shall be handled professionally and within a specified schedule.

4.3 FIELD QUALITY CONTROL

4.3.1 General

Quality control services shall include inspections and tests and related actions including reports.

4.3.2 Installation of Products

Comply with manufacturer's instructions and recommendations for installation of product in the applications indicated.

The Contractor shall be responsible to remedy any defects due to faulty workmanship and materials that appear within one year from the date of acceptance unless Specification sections specify a different duration.

4.4 SYSTEM ACCEPTANCE TEST

4.4.1 Testing

A system acceptance test shall be developed and documented by the Contractor. The Contractor shall perform the tests in the presence of the owner or his designee and document the results.

4.5 SYSTEM DOCUMENTATION

4.5.1 Complete documentation, including 2 hard copies and one electronic copy, shall be provided with the system. The documentation shall completely describe all operations, hardware, and peripherals. The documentation shall at a minimum include an on-line HTML help system for system administrators, managers, and guards. Waukesha County reserves the right to copy documentation for internal use only.

4.6 SYSTEM TRAINING

4.6.1 Proposal shall include pricing to receive system training on-site by a representative of the SMS contractor for system administrators (2), managers (2), and guards (2). Two hard copies and one electronic copy of training manuals for system administrators, managers, and guards shall be provided. Waukesha County reserves the right to copy manuals for internal use only.

o